UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,386	09/18/2003	Radia J. Perlman	SMY-264.01 (25087-26401)	4209

45774 7590 01/17/2007

CHAPIN INTELLECTUAL PROPERTY LAW, LLC
WESTBOROUGH OFFICE PARK
1700 WEST PARK DRIVE
WESTBOROUGH, MA 01581

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/17/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/665,386	PERLMAN, RADIA J.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-44 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-44 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 18 September 2003 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 7/23/04; 4/11/05; 11/23/05.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-44 is pending.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher, et al. (US 6,278,783), and further in view of Filip-Martin, et al. (US 7,082,536).

As per claim :

Kocher discloses a method for performing blinded ephemeral decryption of a message, the method comprising the steps of:

receiving from a first node at an ephemerizer an ephemeral key ID and a message blinded and encrypted with an ephemeral encryption key of an ephemeral key pair to form a blinded and encrypted message **(col.2, lines 26-43 and col.6, lines 39-55)**, said ephemeral key pair; **(col.7, lines 1-8)**

decrypting said blinded and encrypted message using an ephemeral decryption key of said ephemeral key pair to form a blinded message; **(col.4,**

lines 50-55 and col.6, lines 65-66)communicating said blinded message to said first node; and **(col.9, lines 1-15)**

However, Kocher did not discuss said ephemeral key ID and irretrievably deleting said ephemeral decryption key in response to a specified event.

Filip-Martin discloses a system and method for transmitting encrypted messages between an internal user or member of an internal system to an external recipient (col.2, lines 26-29). Filip-Martin discloses creates an encryption key pair, stores them, and encrypts the message with the key pair and transmit a message to the recipient whereby a proper decryption of the key pair is necessary to decrypt the message (col.2, lines 33-41). Filip-Martin discusses message ID that is associated with a key pair where the key pair is in the form of the ephemeral key because the key pair can expire (col.3, lines 37-39 and col.9, lines 22-23). Filip-Martin discloses the server performs a key pair look-up based on the message ID and retrieves the key pair to decrypt the key pair and the message (col.9, lines 18-21). Thus, it is obvious to include an ephemeral key ID of Filip-Martin with the ephemeral key of Kocher because the ID helps refers to the ephemeral key during the look-up in order for decryption (col.9, lines 11-28). Filip-Martin further discusses the claimed irretrievably deleting said ephemeral decryption key where the key pair can be destroyed after a prescribed period of time in response to the deletion instructions which is a specified event (col.3, lines 34-35). The message lifetime value indicates when the encryption key pair is to be deleted upon expiration of the lifetime

value associated with the electronic message so that upon expiration of the lifetime value, the message cannot be decrypted and is unavailable (col.2, lines 48-50 and col.3, lines 36-40). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of Kocher with the teaching of Filip-Martin to irretrievably deleting said ephemeral decryption key in response to a specified event because the expiration period for the message provides the deleting of the key pair so that the decryption of the message with the key pair is not subsequently possible (col.2, lines 58-61).

As per claim 2: See Kocher on col.1, lines 38-40 and col.7, lines 1-8; discussing the method of claim 1 wherein said ephemeral key ID is associated with an ephemeral RSA public and private key pair corresponding to said ephemeral encryption key and said ephemeral decryption key, respectively.

As per claim 3: See Kocher on col.1, lines 18-25 and 38-40; discussing the method of claim 1 wherein said ephemeral key ID is associated with an ephemeral Diffie-Hellman key pair having a public key and a private key corresponding to said ephemeral encryption key and said ephemeral decryption key, respectively.

As per claim 4: See Kocher on col.1, lines 18-25 and col.4, lines 50-54; discussing the method of claim 1 wherein said ephemeral key ID is associated with a secret ephemeral encryption key and a secret ephemeral decryption key and wherein said secret ephemeral encryption key and said secret ephemeral

decryption key are symmetric keys.

As per claim 5: See Kocher on col.4, lines 50-54 and col.6, lines 65-67; discussing the method of claim 1 further including prior to the receiving step, the step of generating said ephemeral key ID and said ephemeral encryption and decryption keys of said ephemeral key pair.

As per claim 6: See Kocher on col.6, lines 39-55 and Filip-Martin on col.2, lines 33-41; discussing the method of claim 5 further including the steps of: receiving a request for an ephemeral encryption key from said first node; and providing said ephemeral key ID and said ephemeral encryption key of said ephemeral key pair to said first node.

As per claim 7: See Kocher on col.6, lines 39-55 and Filip-Martin on col.2, lines 33-35; discussing the method of claim 6 further including the steps of: encrypting a message by said first node using said ephemeral encryption key to form an encrypted message; securely transmitting said encrypted message to a second node.

As per claim 8: See Filip-Martin on col.2, lines 33-34; discussing the method of claim 6 further including the steps of: encrypting said message by said first node using said ephemeral encryption key to form an encrypted message; and securely storing said encrypted message by a second node.

As per claim 9: See Kocher on col.2, lines 64-66; discussing the method of claim 8 further including the step of: retrieving said securely stored encrypted message by said second node.

As per claim 10: See Kocher on col.6, lines 39-55 and Filip-Martin on col.2, lines 33-35; discussing the method of claim 8 wherein the second node and the first node are the same node.

As per claim 11: See Kocher on col.1, lines 18-25 and 38-40; discussing the method of claim 5 wherein said ephemeral encryption key and said ephemeral decryption key of said ephemeral key pair are an ephemeral RSA public key and corresponding private key, respectively.

As per claim 12: See Kocher on col.1, lines 18-25 and 38-40; discussing the method of claim 5 wherein the ephemeral encryption key and said ephemeral decryption key of said ephemeral key pair are Diffie-Hellman public and private keys, respectively.

As per claim 13: See Kocher on col.1, lines 18-25 and col.7, lines 1-8; discussing the method of claim 5 wherein said ephemeral encryption key and said ephemeral decryption key of said ephemeral key pair are secret symmetric encryption and decryption keys.

As per claim 14: See Kocher on col.14, lines 5-25; discussing the method of claim 5 further including the step of storing said generated ephemeral decryption key on a smart card.

As per claim 15: See Filip-Martin on col.2, lines 48-61 and col.3, lines 36-40; discussing the method of claim 14 further including the step of irretrievably deleting said ephemeral key stored on said smart card in response to a specified event.

As per claim 16: See Filip-Martin on col.2, lines 48-61 and col.3, lines 36-40; discussing the method of claim 15 further including the step of physically destroying said smart card in response to a specified event.

As per claim 17: See Filip-Martin on col.3, lines 34-40; discussing the method of claim 1 wherein said specified event is the recognition of a predetermined date and time.

As per claim 18: See Filip-Martin on col.3, lines 30-40; discussing the method of claim 1 wherein said specified event is in response to a request by a user to delete said ephemeral decryption key.

As per claim 19:

Kocher discloses a method for performing blind ephemeral decryption of a message M that has been encrypted to form an encrypted message, comprising the steps of:

in a first blinding step, blinding said encrypted message at a first node with a blinding function z to form a first blinded and encrypted message, wherein z has an inverse z.sup.-1; **(col.2, lines 26-43 and col.6, lines 39-55)**

in a first communicating step, communicating said first blinded and encrypted message from said first node to a decryption agent;

decrypting said first blinded and encrypted message by said decryption agent using an ephemeral decryption function **(col.7, lines 1-8)** to form a first blinded message, wherein said ephemeral decryption function is the inverse of said ephemeral encryption function;

in a second communicating step, communicating said first blinded message from said decryption agent to said first node; and **(col.4, lines 50-55 and col.9, lines 1-15)**

in a first unblinding step, unblinding said first blinded message using z.sup.-1, to obtain said message M; and **(col.6, lines 52 and 65-66)**

However, Kocher did not discuss irretrievably deleting said ephemeral decryption key in response to a specified event.

Filip-Martin discloses a system and method for transmitting encrypted messages between an internal user or member of an internal system to an external recipient (col.2, lines 26-29). Filip-Martin discloses creates an encryption key pair, stores them, and encrypts the message with the key pair and transmit a message to the recipient whereby a proper decryption of the key pair is necessary to decrypt the message (col.2, lines 33-41). Filip-Martin further discusses the claimed irretrievably deleting said ephemeral decryption key where the key pair can be destroyed after a prescribed period of time in response to the deletion instructions which is a specified event (col.3, lines 34-35). The message lifetime value indicates when the encryption key pair is to be deleted upon expiration of the lifetime value associated with the electronic message so that upon expiration of the lifetime value, the message cannot be decrypted and is unavailable (col.2, lines 48-50 and col.3, lines 36-40). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of Kocher with the

teaching of Filip-Martin to irretrievably deleting said ephemeral decryption key in response to a specified event because the expiration period for the message provides the deleting of the key pair so that the decryption of the message with the key pair is not subsequently possible (col.2, lines 58-61).

As per claim 20: See Kocher on col.4, lines 50-55 and col.14, lines 25-30; discussing the method of claim 19 wherein said first node and said decryption agent are communicably coupled via a network, and at least one of said first and second communicating steps comprises the step of communicating the respective message over said network.

As per claim 21: See Kocher on col.14, lines 25-30; discussing the method of claim 20 wherein said first and second communicating steps comprise communicating the respective messages over said network.

As per claim 22: See Kocher on col.4, lines 50-55 and col.9, lines 1-15; discussing the method of claim 19 wherein said first communicating step comprises the step of communicating said first blinded and encrypted message from said first node to said decryption agent via an anonymizer node and said second communicating step comprises the step of communicating said first blinded message from said decryption agent to said first node via said anonymizer node.

As per claim 23: See Filip-Martin on col.3, lines 34-40; discussing the method of claim 19 further including the step of rendering said ephemeral decryption function irretrievably deleted upon the occurrence of said specified

event.

As per claim 24: See Filip-Martin on col.3, lines 3-10; discussing the method of claim 19 further including the step of generating said message at said first node.

As per claim 25: See Kocher on col.2, lines 26-42 and col.7, lines 1-8; discussing the method of claim 17 wherein said ephemeral encryption and decryption functions are respectively, ephemeral public and private keys of an ephemeral public key pair.

As per claim 26: See Kocher on col.1, lines 38-42 and col.7, lines 1-8; discussing the method of claim 25 wherein said ephemeral public and private keys comprise an ephemeral RSA public/private key pair of the form (e,n) and (d,n) respectively.

As per claim 27: See Kocher on col.4, lines 50-55 and col.9, lines 1-15; discussing the method of claim 26 wherein said first blinding step, said blinding function, z, is a number R having an inverse R.sup.-1 that satisfies R*R.sup.-1=1 mod n and wherein said blinding step includes the step of forming the first blinded and encrypted message as the product (R.sup.e*M.sup.e mod n) where (M.sup.e mod n) is said message M encrypted using said ephemeral public encryption key.

As per claim 28: See Kocher on col.4, lines 50-55 and col.9, lines 1-15; discussing the method of claim 27 wherein the decryption step includes the step of raising the product ((R.sup.e*M.sup.e) mod n) to the power d mod n,

forming ((R.sup.e*M.sup.e) mod n)).sup.d mod n to form said first blinded message R*M mod n.

As per claim 29: See Kocher on col.4, lines 50-55 and col.9, lines 1-15; discussing the method of claim 28 wherein the first unblinding step includes the step of unblinding said first blinded message R*M mod n using R.sup.-1 to obtain said message M.

As per claim 30: See Kocher on col.2, lines 34-38 and col.4, lines 47-55; discussing the method of claim 27 further including the step of generating an integer random number and utilizing said random number as the blinding number R.

As per claim 31: See Kocher on col.1, lines 38-42 and col.4, lines 47-55; discussing the method of claim 19 further comprising the steps of: obtaining an ephemeral public key associated with said decryption agent, wherein said ephemeral public key is a Diffie-Hellman public key of the form g.sup.x mod p; selecting a blinding number y having an inverse blinding number y.sup.-1 that satisfies y*y.sup.-1=1 mod p-1; raising said public key g.sup.x mod p to the power y to obtain g.sup.xy mod p; raising g to the power y to form g.sup.y mod p; encrypting said message M using g.sup.xy mod p to form an encrypted message of the form {M}g.sup.xy mod p; storing a copy of said encrypted message {M}g.sup.xy mod p; and storing a copy of g.sup.y mod p.

As per claim 32: See Kocher on col.6, lines 53-65 and col.9, lines 1-15; discussing the method of claim 31 wherein the step of decrypting said blinded

and encrypted message by said first node includes the steps of: selecting a blinding number, w having an inverse blinding function w.sup.-1 that satisfies w*w.sup.-1=1 mod p-1; raising said ephemeral public key g.sup.x mod p to the power w to obtain g.sup.yw mod p; forwarding g.sup.yw mod to said decryption agent; receiving g.sup.xyw mod p from said decryption agent; raising g.sup.xyw mod p to the inverse blinding number, w.sup.-1, to form g.sup.xy mod p; and decrypting said encrypted message {M}g.sup.xy mod p using g.sup.xy mod p to obtain said message M.

As per claim 33: See Kocher on col.2, lines 34-38 and col.4, lines 47-55; discussing the method of claim 31 wherein y is a randomly selected integer.

As per claim 34: See Kocher on col.2, lines 34-38; discussing the method of claim 31 wherein w is a randomly selected integer.

As per claim 35: as rejected in claim 19; discussing the method of claim 19 including, prior to said first blinding step, the steps of: selecting a blinding number y having an inverse blinding number y.sup.-1; in a second blinding step, blinding said message M using said blinding number y to form a second blinded message; forwarding said second blinded message to an encryption agent; encrypting by said encryption agent said second blinded message to form a second blinded and encrypted message, wherein said ephemeral encryption is performed using said ephemeral encryption function and wherein said ephemeral encryption function and said corresponding ephemeral decryption function are secret symmetric ephemeral encryption and ephemeral

decryption keys, respectively; forwarding said second blinded and encrypted message from said encryption agent to said first node; and in a second unblinding step, unblinding said second blinded and encrypted message using said inverse blinding number y.sup.-1 to form said encrypted message.

As per claim 36: See Kocher on col.2, lines 26-42; discussing the method of claim 35 wherein said second blinding step includes the step of raising said message M to the power y mod p.

As per claim 37: See Kocher on col.2, lines 26-42 and col.7, lines 1-8; discussing the method of claim 36 wherein said secret symmetric ephemeral encryption key is a value x and wherein said secret symmetric ephemeral decryption key is x.sup.-1 and wherein said step of encrypting said second blinded message includes the step of raising said second blinded message M.sup.y mod p to the power x mod p to form said second blinded and encrypted message.

As per claim 38: See Kocher on col.4, lines 50-55 and col.9, lines 1-15; discussing the method of claim 37 wherein second unblinding step, includes the step of raising said second blinded and encrypted message M.sup.xy mod p to the power y.sup.-1 mod p, to obtain said encrypted message M.sup.x mod p.

As per claim 39: See Kocher on col.4, lines 50-55 and col.9, lines 1-15; discussing the method of claim 38 wherein the step of decrypting said first blinded and encrypted message by said decryption agent includes the step of raising said first blinded and encrypted message to said secret ephemeral

decryption key x.sup.-1 to form a first blinded message M.sup.z mod p.

As per claim 40: See Filip-Martin on col.3, lines 34-40; discussing the method of claim 23 wherein said specified event is the occurrence of a predetermined date and time.

As per claim 41: See Filip-Martin on col.2, lines 48-61 and col.3, lines 35-40; discussing the method of claim 23 wherein said specified event includes a request by a user to delete said ephemeral decryption key.

As per claims 42 and 43:

Kocher discloses a system for performing blinded ephemeral decryption of a message, the system comprising:

an ephemerizer communicably coupled to a first node via a communications network; **(col.2, lines 2-5 and col.14, lines 25-30)**

the ephemerizer operative to;

receive from said first node a blinded and encrypted message, said message being encrypted with an encryption key having a corresponding ephemeral decryption key **(col.7, lines 1-8)** and said message being blinded with a blinding function to form said blinded and encrypted message; **(col.2, lines 26-43 and col.6, lines 39-55)**

receive from said first node an ephemeral decryption key; **(col.2, lines 60-67 and col.9, lines 1-15)**

decrypt said blinded and encrypted message using said ephemeral decryption key to form a blinded message; **(col.4, lines 50-55 and col.6, lines 53-55 and 65-66)**

communicate said blinded message to said first node; and **(col.14, lines 25-30)**

However, Kocher did not discuss said ephemeral key ID and irretrievably deleting said ephemeral decryption key in response to a specified event.

Filip-Martin discloses a system and method for transmitting encrypted messages between an internal user or member of an internal system to an external recipient (col.2, lines 26-29). Filip-Martin discloses creates an encryption key pair, stores them, and encrypts the message with the key pair and transmit a message to the recipient whereby a proper decryption of the key pair is necessary to decrypt the message (col.2, lines 33-41). Filip-Martin discusses message ID that is associated with a key pair where the key pair is in the form of the ephemeral key because the key pair can expire (col.3, lines 37-39 and col.9, lines 22-23). Filip-Martin discloses the server performs a key pair look-up based on the message ID and retrieves the key pair to decrypt the key pair and the message (col.9, lines 18-21). Thus, it is obvious to include an ephemeral key ID of Filip-Martin with the ephemeral key of Kocher because the ID helps refers to the ephemeral key during the look-up in order for decryption (col.9, lines 11-28). Filip-Martin further discusses the claimed irretrievably deleting said ephemeral decryption key where the key pair can be destroyed

after a prescribed period of time in response to the deletion instructions which is a specified event (col.3, lines 34-35). The message lifetime value indicates when the encryption key pair is to be deleted upon expiration of the lifetime value associated with the electronic message so that upon expiration of the lifetime value, the message cannot be decrypted and is unavailable (col.2, lines 48-50 and col.3, lines 36-40). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of Kocher with the teaching of Filip-Martin to irretrievably deleting said ephemeral decryption key in response to a specified event because the expiration period for the message provides the deleting of the key pair so that the decryption of the message with the key pair is not subsequently possible (col.2, lines 58-61).

As per claim 44:

Kocher discloses a computer program product including a computer readable medium, said computer readable medium having a computer program stored thereon for use in blinded ephemeral decryption, said computer program being executable on a processor in said ephemerizer comprising:

program code for:

receiving from said first node a blinded and encrypted message, said message being encrypted with an encryption key having a corresponding ephemeral decryption key **(col.2, lines 60-67 and col.7, lines 1-8)** and said

message being blinded with a blinding function to form said blinded and encrypted message; **(col.2, lines 26-43 and col.6, lines 39-55)**

receiving from said first node an ephemeral decryption key; **(col.4, lines 50-55 and col.9, lines 1-15)**

decrypting said blinded and encrypted message using said ephemeral decryption key to form a blinded message; **(col.6, lines 53-55 and 65-66)**

communicating said blinded message to said first node; and **(col.14, lines 25-30)**

However, Kocher did not discuss said ephemeral key ID and irretrievably deleting said ephemeral decryption key in response to a specified event.

Filip-Martin discloses a system and method for transmitting encrypted messages between an internal user or member of an internal system to an external recipient (col.2, lines 26-29). Filip-Martin discloses creates an encryption key pair, stores them, and encrypts the message with the key pair and transmit a message to the recipient whereby a proper decryption of the key pair is necessary to decrypt the message (col.2, lines 33-41). Filip-Martin discusses message ID that is associated with a key pair where the key pair is in the form of the ephemeral key because the key pair can expire (col.3, lines 37-39 and col.9, lines 22-23). Filip-Martin discloses the server performs a key pair look-up based on the message ID and retrieves the key pair to decrypt the key pair and the message (col.9, lines 18-21). Thus, it is obvious to include an ephemeral key ID of Filip-Martin with the ephemeral key of Kocher because the

ID helps refers to the ephemeral key during the look-up in order for decryption (col.9, lines 11-28). Filip-Martin further discusses the claimed irretrievably deleting said ephemeral decryption key where the key pair can be destroyed after a prescribed period of time in response to the deletion instructions which is a specified event (col.3, lines 34-35). The message lifetime value indicates when the encryption key pair is to be deleted upon expiration of the lifetime value associated with the electronic message so that upon expiration of the lifetime value, the message cannot be decrypted and is unavailable (col.2, lines 48-50 and col.3, lines 36-40). Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teaching of Kocher with the teaching of Filip-Martin to irretrievably deleting said ephemeral decryption key in response to a specified event because the expiration period for the message provides the deleting of the key pair so that the decryption of the message with the key pair is not subsequently possible (col.2, lines 58-61).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LH

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100